NCUA RISK ALERT

NATIONAL CREDIT UNION ADMINISTRATION
1775 Duke Street, Alexandria, VA 22314

DATE: 2009 **RISK ALERT NO.: 09-Risk-01**

TO: Federally Insured Credit Unions

SUBJ: Information Systems & Technology Application Security

ENCL: Information Systems & Technology Application Security

Dear Board of Directors:

This Alert emphasizes the importance of application security as a key component of an information security program for credit union management and technology service providers.[1] Application security, as used in this Alert, refers to the creation, acquisition, and maintenance of software that is substantially free of vulnerabilities and supports the products and services of a credit union. Operating systems, generic office products, and other non-credit union software are not considered as part of this Alert.

In 2008, the number of electronic records breached was more than the combined amount for the previous four years.[2] The financial sector accounted for 93 percent of all the records compromised last year. Organized crime was implicated by law enforcement in 90 percent of the records breached. Nearly all the records compromised were from online assets and while there is concern over mobile devices and portable media, 99 percent of all breached records were compromised from applications and servers. Application security, application testing, and application code review have never been more important to protect critical credit union member data and assets.

---

[1] Technology service providers generally include independent third-party processors, joint venture/limited liability corporations, bank service corporations, corporate credit unions, credit union service organizations and other organizations which provide technology-based products to credit unions.

[2] 2009 Verizon Business Data Breach Study at http://www.verizonbusiness.com/us/resources/media/1008a1a3-111=129947-Verizon+Business+2009+Data+Breach+Investigations+Report.xml.

All applications, whether internally developed, vendor-acquired, or contracted by the credit union, need to be subjected to a risk assessment and risk mitigation process. Vulnerabilities in applications increase operational and reputation risks as unplanned or unknown weaknesses in applications may compromise the confidentiality, availability, and integrity of credit union data. While this guidance focuses on the risks and risk mitigation techniques associated with web-based applications, the principles contained in this Alert and Enclosure apply to all types of software utilized by credit unions and technology service providers.

If you have any questions or concerns, please contact your NCUA Regional Office or State Supervisory Authority.

Sincerely,

Michael E. Fryzel
Chairman

Enclosure